UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/725,116	12/02/2003	Victor Gorelik		2789

7590   03/27/2008

Dr. Victor Gorelik
Apt. C1
254 73 Street
Brooklyn, NY 11209

EXAMINER
LOUIE, OSCAR A

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
03/27/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Application Number: 10/725,116
Filing Date: December 02, 2003
Appellant(s): GORELIK, VICTOR

<div style="text-align:center">

Victor Gorelik
Pro Se
Appellant

</div>

<div style="text-align:center">

EXAMINER'S ANSWER

</div>

This is in response to the appeal brief filed 12/06/2007 appealing from the Office action mailed 10/22/2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The following are the related appeals, interferences, and judicial proceedings known to

the examiner which may be related to, directly affect or be directly affected by or have a

bearing on the Board's decision in the pending appeal:

(3) Status of Claims

The statement of the status of claims contained in the brief amendment filed 01/03/2008

is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is as

follows:

Claims 1-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over <u>Buffam</u> (US-

6185316-B1) in view of <u>Scheidt et al.</u> (US-6542608-B2).

See section (vii) Argument, page 3 of Brief.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,185,316   Buffam   02-2001

6,542,608   Scheidt et al.   04-2003

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

1.   Claims 1-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Buffam (US-6185316-B1) in view of Scheidt et al. (US-6542608-B2).

Claim 1:

Buffam discloses a method for securely submitting biometric data from a client to a server comprising,

-   "performing sampling of a real biometric characteristic at the client" [Fig 8 illustrates sampling of biometric characteristics];

but Buffam does not disclose,

-   "shuffling arrays of real biometric characteristics in the sequence known at client only to thereby generate twisted biometric data"

-   "submitting the twisted biometric data from the client to the server"

however, Scheidt et al. do disclose,

- "This information, in digital form, will then be used to generate the biometric split 38. This may be accomplished by, for example, randomizing a digital string corresponding to the biometric vectors 58 with biometric combiner data 60, which may be a digital hash of the user's system identification number or some other identifying data that can be linked to the user's physical data provided by the biometric reader" [column 5 lines 34-41];

- "Referring to FIG. 1, a communication has an origination space 2 and a destination space 4" [column 3 lines 46-47];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "shuffling arrays of real biometric characteristics in the sequence known at client only to thereby generate twisted biometric data" and "submitting the twisted biometric data from the client to the server," in the invention as disclosed by Buffam since it is implied that a submission of "twisted biometric data" would occur between two points an origination space and a destination space, where the randomizing (i.e. shuffling) of a digital string corresponding to biometric vectors (i.e. arrays of real biometric characteristics) with biometric combiner data may be random/pseudorandom and not necessarily hashing.

Claim 2:

Buffam and Scheidt et al. discloses a method for securely submitting biometric data from a client to a server, as in Claim 1 above, but their combination do not disclose,

- "the shuffling sequence is calculated at client on the base of the value of a secret object created at the client and known to client only"

however, Scheidt et al. do disclose,

- "This may be accomplished by, for example, randomizing a digital string corresponding
  to the biometric vectors 58 with biometric combiner data 60, which may be a digital hash
  of the user's system identification number or some other identifying data that can be
  linked to the user's physical data provided by the biometric reader" [column 5 lines 36-
  41];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the

applicant's invention to include, "the shuffling sequence is calculated at client on the base of the

value of a secret object created at the client and known to client only," in the invention as

disclosed by Buffam for the purposes of increased difficulty in determining the randomizing

sequence/method used (i.e. "provides information that is incapable of being reproduced by

anyone but the user providing the biometric data vector") [column 5 lines 42-44].

Claim 3:

Buffam and Scheidt et al. discloses a method for securely submitting biometric data from a client

to a server, as in Claim 2 above, further comprising,

- "the step of multiplying the arrays of biometric characteristics by the sequences of
  numbers fixed for each type of array and known at the client only" (i.e. "Typically, an
  original image is represented by many discrete information points, similar to grid points
  on a map. True image points can be extracted from the information points on the basis of
  pragmatic considerations, such as data reduction. The set of true image points can be
  stored as a master template uniquely representative of the original image. False image

points are generated and are selectively interposed among a chosen subset of the true

image points, forming a transient template. The false image points also may be

transformed to produce an encoding key") [column 12 lines 4-27].

Claim 4:

Buffam and Scheidt et al. discloses a method for securely submitting biometric data from a client

to a server, as in Claim 3 above, further comprising,

- "the step of submitting of twisted biometric data is followed by the step of comparing this

  data against the samples of twisted biometric data saved at the server previously, in such

  a way, that the result of the verification and/or identification depends neither on the

  specific sequence in which biometric arrays were shuffled on the client, nor on the

  specific sequence of numbers used on the client to change the values of the arrays" (i.e.

  "Once the user is enrolled, the biometric is used to verify the user's identity, step 805.

  When claimant 870 needs to be authenticated, a sample 872 of the user's biological

  feature is sensed, digitized, and processed. The digitized sample is compared to the stored

  biometric template, step 875, here stored in credential 860") [column 18 lines 67 &

  column 19 lines 1-2].

Claim 5:

Buffam discloses a method for securely submitting biometric data from a client to a server

comprising,

- "said system programmed for performing verification and/or identification of the client"

  (i.e. "Once the user is enrolled, the biometric is used to verify the user's identity, step

  805. When claimant 870 needs to be authenticated, a sample 872 of the user's biological

feature is sensed, digitized, and processed. The digitized sample is compared to the stored

biometric template, step 875, here stored in credential 860") [column 18 lines 67 &

column 19 lines 1-2];

but <u>Buffam</u> does not disclose,

- "means for performing twisted sampling by changing the sequence of terms in biometric

array and submitting data to the server"

however, <u>Scheidt et al.</u> do disclose,

- "This information, in digital form, will then be used to generate the biometric split 38.

This may be accomplished by, for example, randomizing a digital string corresponding to

the biometric vectors 58 with biometric combiner data 60, which may be a digital hash of

the user's system identification number or some other identifying data that can be linked

to the user's physical data provided by the biometric reader" [column 5 lines 34-41];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the

applicant's invention to include, "means for performing twisted sampling by changing the

sequence of terms in biometric array and submitting data to the server," in the invention as

disclosed by <u>Buffam</u> since it is implied that a submission of "twisted biometric data" would

occur between two points an origination space and a destination space, where the randomizing

(i.e. shuffling/twisting) of a digital string corresponding to biometric vectors (i.e. arrays of real

biometric characteristics) with biometric combiner data may be random/pseudorandom and not

necessarily hashing.

(10) Response to Argument

The appellant's arguments are directed to invention aspects described in the instant specification and not the claim language claim. The appellant recites overall goals and summaries of the prior art of record, and compares them to explicitly detailed limitations found in the appellant's specification but not in the claims. The appellant has not shown that the prior art of record is deficient in being obvious over the claims language.

In particular, the applicant's claim language for independent Claim 1 recites, "performing sampling of a real biometric characteristic at the client," "shuffling arrays of real biometric characteristics in the sequence known at client only to thereby generate twisted biometric data," and "submitting the twisted biometric data from the client to the server," where Fig 8 of Buffam illustrates sampling of biometric characteristics (i.e. "performing sampling of a real biometric characteristic at the client") and Scheidt et al. disclose, "This information, in digital form, will then be used to generate the biometric split 38. This may be accomplished by, for example, randomizing a digital string corresponding to the biometric vectors 58 with biometric combiner data 60, which may be a digital hash of the user's system identification number or some other identifying data that can be linked to the user's physical data provided by the biometric reader" [column 5 lines 34-41] (i.e. "shuffling arrays of real biometric characteristics in the sequence known at client only to thereby generate twisted biometric data" and "submitting the twisted biometric data from the client to the server").

The appellant has not addressed the above claim limitations directly. The appellant states, "A. Goal of invention. Buffam is concerned with security of the server and does not use word "privacy" in his invention at all. Scheidt uses the word "privacy", but in different sense

than I do," which fails to address the claim limitation covered by <u>Buffam,</u> "performing sampling

of a real biometric characteristic at the client." The appellant also states, "B. <u>Buffam's</u> method

vs, my method. <u>Buffam</u> uses true and false image points in his encoding procedure. The

claimant receives access to the server only if he or she provides correct (real) biometric data and

correct plain text (password known to the user only). So, if the system lets the attacker in, he or

she knows that submitted/generated biometric data is real. Using method of trial and error the

attacker can restore this data and use it for purposes other then access to this particular server,"

which again does not address the limitations found in the appellant's claim language.

In regards to the prior art of record, <u>Schedit et al.,</u> the appellant states, "C. <u>Scheidt's</u>

method vs. my method. Unlike <u>Buffam,</u> <u>Scheidt</u> randomizes a digital string corresponding to the

user's biometric vector. It is also different from my shuffling of terms in the biometric vector

with multiplying these terms by some numbers. My method has an advantage from the point of

view of the user's privacy for the following reasons," which does not address the claim

limitations found in the claims language, "shuffling arrays of real biometric characteristics in the

sequence known at client only to thereby generate twisted biometric data" and "submitting the

twisted biometric data from the client to the server."

In addition, the appellant states, in regard to the combination of <u>Buffam</u> and <u>Scheidt et</u>

<u>al.,</u> "D. <u>Buffam's</u> method in view of <u>Scheidt's</u> method vs. my method. <u>Buffam</u> and <u>Scheidt</u> do

not teach or suggest my proposed invention. As has been shown above, protection of the privacy

of the user's biometrical information in case of a server security breach is not the focus of

<u>Buffam's</u> and <u>Scheidt's</u> inventions and they do not accomplish this goal. Neither does the

combination, as shown in the following simplified example, fig8-fig9," which once again does

not address the actual limitations found in the appellant's claims language.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related

Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/OAL/
Oscar A. Louie
03/19/2008

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132

Conferees:

/G.B.J./
Gilberto Barron, SPE 2132

Benjamin Lanier
/Benjamin E Lanier/
Primary Examiner, Art Unit 2132